

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for the Premises Known and Described as 43-07 42nd Street, Apartment 3A, Sunnyside, NY 11104 and Any Closed Containers/Items Contained Therein

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

20 M 063

EASTERN DISTRICT OF NEW YORK) ss.:

Kerwin John, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent with the Department of Justice, Office of Inspector General (“DOJ-OIG”). As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with DOJ-OIG since September 2008. In that capacity I have been involved in investigations of criminal and administrative misconduct by DOJ personnel as well as allegations of waste, fraud, and abuse regarding DOJ personnel and programs. I am currently assigned to DOJ-OIG’s Cyber Investigations Office. Through my training, education and experience, I have become familiar with the manner in which criminal activity is carried out, and the efforts of persons involved in such activity to avoid detection by law enforcement.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the “Subject Premises”) for, and to seize, the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my

conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises is located at 43-07 42nd Street, Apartment 3A, Sunnyside, New York, 11104, which is a multi-story residential apartment building located on 42nd Street, between 43rd Avenue and Queens Boulevard in Sunnyside, Queens (the “Building”). The building has a brick exterior with windows on each floor with the number “43-07” in gold writing affixed to the outside of the front entrance of the building. The Subject Premises is located on the third floor of the building. The entrance to the Subject Premises is a tan door with the alphanumeric characters “3A” affixed to it, which is accessible from the third floor hallway. A photograph of the entrance of the Subject Premises is depicted below:



C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises contains evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (attempted production of child pornography), 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity), 2252A(a)(5)(B) (attempted possession of child pornography), and 2252A(a)(2)(B) (attempted receipt of child pornography) (the “Subject Offenses”).

II. Probable Cause

A. Probable Cause Regarding Subject’s Commission of the Subject Offenses

Investigation Background

5. Based on my conversations with other witnesses, law enforcement officers, my review of documents and recorded communications, my involvement in this investigation, and my training and experience, I have learned the following, among other things:

a. The New York City Police Department (the “NYPD”) and the DOJ-OIG (together, the “Investigating Agencies”) have been investigating FREDERICK SCHEININ for violations of the Subject Offenses. SCHEININ currently works for the Drug Enforcement Administration (the “DEA”) in New York, New York, as a diversion investigator.

b. In an effort to detect and apprehend perpetrators of child exploitation offenses, law enforcement officers working with the NYPD have occasionally operated an undercover Grindr account (the “UC Grindr Account”). Based on my participation in this investigation, I am aware that Grindr is a social networking and online dating application that primarily markets to the gay, bi-sexual, transgender, and queer community. Grindr’s terms of service prohibit children below the age of eighteen from creating or using Grindr accounts. However, based on my participation in this investigation and my communications with other law

enforcement officers, I am aware that minors frequently use Grindr to communicate with and meet others. Due to Grindr's terms of service, the UC Grindr Profile listed the user's age as eighteen, but the law enforcement officers who operated the UC Grindr Account typically told individuals who communicated with the UC Grindr Account that the operator of the UC Grindr Account was fourteen years old.

c. Beginning in or around October 2019, an individual believed to be SCHEININ began communicating with the UC Grindr Account. The law enforcement officers operating the UC Grindr Account told SCHEININ, in substance and in part, that the user of the UC Grindr Account was fourteen years old. On or about October 26, 2019, SCHEININ sent his phone number, 631-236-7220 (the "Scheinin Phone Number"), to the UC Grindr Account.

Scheinin's Communications with a Fictitious Minor

6. Based on my conversations with other witnesses, law enforcement officers, my review of documents and recorded communications, my involvement in this investigation, and my training and experience, I have learned the following, among other things:

a. Beginning on or about October 26, 2019, SCHEININ began communicating with an undercover law enforcement officer ("UC-1")¹ using Google Voice text messaging application that was associated with the Scheinin Phone Number. During that text exchange, SCHEININ asked UC-1, among other things, "So when are we gonna chill?"

b. On or about October 29, 2019, SCHEININ and UC-1 again communicated using Google Voice text messaging. During this text exchange, SCHEININ stated that he lived in "Sunnyside." SCHEININ asked where UC-1 lived, and UC-1 responded, in substance and in part,

¹ UC-1 is used herein to refer to one of several law enforcement officers who used various digital communication applications to communicate with SCHEININ.

that UC-1 lived with UC-1's mother in Whitestone. SCHEININ then asked UC-1, "are you far from the 7 in flushing?" UC-1 then asked, "what's that," and SCHEININ responded, "lol the subway." UC-1 told SCHEININ that UC-1 does not take the subway.

c. On or about November 6, 2019, SCHEININ and UC-1 again communicated using Google Voice text messaging. When UC-1 asked for his name, SCHEININ responded that his name was "Zach." SCHEININ stated that he was 29 years old. In response, UC-1 stated, "Oh ok im 14." SCHEININ responded, "alright." Later in the text exchange, UC-1 told SCHEININ that high school "sucks."

d. On or about November 7, 2019, using Google Voice text messaging, SCHEININ and UC-1 discussed communicating through Snapchat's video chat function. Based on my involvement in this investigation, I am aware that Snapchat is a messaging application that offers its users the ability to communicate with each other through text messaging and real time video chat. Photos and text messages sent through Snapchat are usually only available for a short time before they become inaccessible to their recipients. For purposes of this investigation, law enforcement photographed, recorded, or otherwise memorialized Snapchat messages between SCHEININ and UC-1. During this November 7 text exchange, SCHEININ sent his Snapchat username, Zachs6015 (the "SCHEININ Snap Username"), to UC-1.

e. On or about November 8, 2019, SCHEININ and UC-1 communicated in real time using Snapchat's video chat. During this communication and all other video communications with SCHEININ, UC-1's appearance was partially disguised to be consistent with that of a fourteen year-old boy. During this November 8, 2019 video chat communication, SCHEININ stated, in substance and in part, that he was home in his bedroom and asked UC-1 for how long UC-1 would be home alone. Later during this video chat, UC-1 asked SCHEININ, "so

you like don't care that I'm younger?" SCHEININ responded, "No, it's cool. As long as you're cool with it." Approximately one minute later, SCHEININ asked UC-1, "have you ever like done anything on snapchat before, you know, like, jerked off with someone or anything like that?" SCHEININ then stated, in substance and in part, that he had masturbated on Snapchat and that it was "all right" but that "it's better in person."

f. On or about November 19, 2019, SCHEININ and UC-1 communicated using Snapchat's text messaging feature. UC-1 told SCHEININ, in substance and in part, that UC-1's father would soon be moving to an apartment in Manhattan. UC-1 stated that UC-1 was excited because UC-1 would "get to take the train in like by my self."

g. On or about December 4, 2019, UC-1 sent SCHEININ the text message, "hey," through the Google Voice application. A short time after this text message was sent on December 4, SCHEININ responded through Snapchat: "Got your text before. I think it's better we chat on here." Based on the context of this conversation and my participation in this investigation, I believe SCHEININ directed UC-1 to communicate through Snapchat only (as opposed to text message) because Snapchat communications are automatically deleted.

h. On or about December 11, 2019, UC-1 and SCHEININ communicated using Snapchat's text messaging feature. UC-1 told SCHEININ, in substance and in part, that UC-1's father was moving to Manhattan. On or about December 18, 2019, SCHEININ asked UC-1 what part of Manhattan UC-1's father was moving to, and UC-1 responded, "I think lower."

i. On or about December 19, 2020, using Snapchat UC-1 sent a photograph to SCHEININ of UC-1 on the subway. SCHEININ responded, "Where are you heading?" UC-1 responded, "Dads place," which was a reference to UC-1's father's apartment in Manhattan. SCHEININ then asked if UC-1 was alone on the train and then stated, "well maybe one day you

can take it to me lol. I'm right off the seven," a reference to UC-1 taking the subway to meet SCHEININ at the Subject Premises.

j. On or about December 19, 2019, SCHEININ and UC-1 communicated in real time using Snapchat's video chat feature. UC-1 had this conversation from a room in DOJ-OIG's Manhattan offices that was refurbished to appear as a child's bedroom (the "UC-1 Bedroom"). Based on my review of the video recording of this conversation, SCHEININ appeared to be home in his bedroom at the time. During this video chat, SCHEININ asked UC-1, "what are you doing under your blanket there?" Later in the conversation, SCHEININ told UC-1, "maybe one day I'll see you out from under the blanket," and then UC-1 and SCHEININ discussed, in substance and in part, meeting in person. Specifically, UC-1 stated that UC-1 is "usually free after school."

k. On or about the evening of December 20, 2019, SCHEININ and UC-1 had multiple real time communications using Snapchat's video chat feature. At the time of these video chats, UC-1 was located in the UC-1 Bedroom in Manhattan and, based on my review of the video recording of this conversation, SCHEININ appeared to be in his home bedroom. In between one of these video chats, SCHEININ sent UC-1 a photograph of his erect penis. SCHEININ then said to UC-1, "you should send me a pic before you go to bed." UC-1 asked SCHEININ, "pic of what" and SCHEININ responded, "surprise me." Later that evening, SCHEININ used snapchat to send UC-1 multiple pictures of SCHEININ holding his erect penis. Following the transmission of these photographs, SCHEININ and UC-1 exchanged the following Snapchat text messages, in sum and substance:

SCHEININ:	Let me see yours
SCHEININ:	I promise not to judge if that's what you're nervous about.

SCHEININ:	I Don't care about size or hair or anything else like that lol
UC-1:	Im sorry I just feel awkward rite now bc my mom is in the room next to mine. U prob think im a loser.
SCHEININ:	Nooo
SCHEININ:	If I send you another one maybe that will change your mind

SCHEININ then sent UC-1 another picture of his erect penis.

l. Later in the evening of on or about December 20, 2019, UC-1 and SCHEININ again communicated using Snapchat text messaging. UC-1 stated, "Im thinkin of wat I should send." UC-1 and SCHEININ then exchanged the following Snapchat text messages, in substance and in part:

SCHEININ:	Send me what I sent you.
UC-1:	Wat
SCHEININ:	From before lol
UC-1:	The dick pic?
SCHEININ:	Yah

m. On or about January 3, 2020, SCHEININ and UC-1 communicated using Snapchat text messaging. During this text exchange, SCHEININ asked UC-1, "Can you do me a favor? Can you delete our texts out of your phone? You know, just in case she goes crazy and decides to look through your text messages lol. . . . That's why I like Snapshat. It always deletes everything immediately lol" SCHEININ then asked UC-1, "when are we gonna chill lol." UC-1 responded, "Deftly soon."

n. On or about January 7, 2020, SCHEININ and UC-1 communicated in real time using Snapchat's video chat feature. At the time, UC-1 was in the UC-1 Bedroom in Manhattan. During this conversation, SCHEININ requested multiple times that UC-1 take photos of UC-1's penis and send the photos to SCHEININ over Snapchat and/or that UC-1 show UC-1's

penis to SCHEININ over Snapchat's video chat. In response to SCHEININ's requests, UC-1 stated, "I kinda want to," and SCHEININ responded, "I think you should. Just really quick." UC-1 and SCHEININ then engaged in the following colloquy, in substance and in part:

UC-1:	Well, I'm not ready right now . . . because it's soft. So I don't know if you'd wanna see it soft.
SCHEININ:	Well, I'll see it soft first and then see what happens.
UC-1:	So you don't care if it's hard or soft?
SCHEININ:	I mean, I think I'd like to see it both ways and then I'll see which way I like it better.
UC-1:	I don't know yet. I have to feel more comfortable first.
SCHEININ:	All right. That's cool.
UC-1:	I'm still nervous.
SCHEININ:	What are you nervous about?
UC-1:	I Don't know. Because we haven't met yet in person. Does that bother you?
SCHEININ:	No. But I still want to see it.

o. During the January 7 conversation, UC-1 and SCHEININ discussed their sexual preferences and, in that context, SCHEININ stated, in sum and substance, "I would prefer to take control." SCHEININ then asked about UC-1's preferences, and UC-1 stated, "I guess I would do whatever . . . it's up to you type of thing." SCHEININ responded, "all right. Sounds good."

p. On or about January 9, 2020, SCHEININ and UC-1 communicated in real time using Snapchat's video chat feature. UC-1 had this conversation from the UC-1 Bedroom in Manhattan and, based on my review of a video recording of this conversation, SCHEININ appeared to be home in his bedroom. During this video chat, SCHEININ showed his penis and then stated, in substance and in part, "I kinda want to see what's under those boxers. . . . I just want to see it. I think it's hot." Shortly thereafter, SCHEININ said, in sum and substance, "stop

being shy,” and in reference to UC-1’s penis, SCHEININ asked, in sum and substance, “why don’t you touch it.” In response, UC-1 asked, “do I have to?” and SCHEININ responded, “uh-huh.” Based on my review of the video recording of this conversation, I am aware that SCHEININ began masturbating on the video chat—SCHEININ displayed his hand stroking his erect penis. During or around the time he was masturbating, SCHEININ then repeatedly asked UC-1, in substance and in part, to transmit a live visual depiction of UC-1’s penis. More specifically, SCHEININ stated, in substance and in part:

- “I want to see it now.”
- “Just show it to me, and then you can put it back.”
- “Don’t be like a pussy.”
- “You know you want to.”
- “You need to pull your boxers down.”

q. During the January 9, 2020 video chat between SCHEININ and UC-1, SCHEININ and UC-1 discussed meeting in person on a later date. UC-1 asked what UC-1 and SCHEININ would do when they met up. SCHEININ stated, in sum and substance, that they would “see what happens.” UC-1 told SCHEININ, in sum and substance, that UC-1’s father would be traveling the week of January 19 and that UC-1 may be alone in the apartment. SCHEININ responded, in sum and substance, that he could meet UC-1 in Manhattan in the afternoon when UC-1 gets home from school. UC-1 asked SCHEININ to bring condoms and lube to the in-person meeting because UC-1 was afraid of getting a disease and did not want to be in any pain. SCHEININ stated, in sum and substance, that he would bring condoms and lubricant to the in-person meeting. SCHEININ then continued to ask UC-1 to send photographs or a live video of UC-1’s penis. SCHEININ stated, in sum and substance, that he wanted the pictures and/or video

because he wanted “something to think about while jerking off.” SCHEININ later said during this conversation that SCHEININ would think about “playing” with and “sucking” UC-1’s penis.

r. Towards the end of the January 9 video chat, SCHEININ said, in sum and substance, “I think I have to jerk off now because this is not going away. . . . I think you should show me really quick before you go.” UC-1 responded, in sum and substance, that UC-1 was too nervous to send a photograph of UC-1’s penis, but UC-1 did not want SCHEININ to forget about UC-1. In an apparent effort to (again) induce UC-1 to send visual depiction of UC-1’s penis, SCHEININ responded, in sum and substance, “I don’t know. What If I find like a new cute boy to talk while I’m soo horny right now.”

s. On or about January 14, 2020, SCHEININ and UC-1 communicated using Snapchat’s text messaging and video chat functions. UC-1 told SCHEININ, in sum and substance, that UC-1 was traveling into the City from Queens and SCHEININ stated, “You should make a pit stop in sunnyside before heading into the city,” which, in this context, was a reference to making a “pit stop” at the Subject Premises. UC-1 stated, in sum and substance, that UC-1 was going to UC-1’s father’s apartment in Manhattan, SCHEININ responded, in sum and substance, “Just tell him you were hanging out with some friends in flushing after school lol.” SCHEININ and UC-1 then discussed, in substance and in part, meeting in person on January 16, 2020. UC-1 and SCHEININ agreed to meet at a particular location in downtown Manhattan (“Location-1”).

Scheinin Meets UC-1 To Engage In Sexual Activity

7. Based on my conversations with other witnesses, law enforcement officers, my review of documents and recorded communications made in the course of this investigation, my involvement in this investigation, and my training and experience, I am aware of the following, among other things:

a. On or about January 15, 2020, SCHEININ and UC-1 communicated using Snapchat's video chat feature. During this video chat, UC-1 was outside, standing on a sidewalk in Manhattan. UC-1 stated, in sum and substance, that UC-1 was standing outside of a restaurant and that UC-1's father was inside of the restaurant. SCHEININ confirmed, in sum and substance, that UC-1's father would not be home the following day. SCHEININ stated, in sum and substance, that he could meet UC-1 around 5:00 p.m. the following day. UC-1 asked SCHEININ if SCHEININ was going to bring lubricant, and SCHEININ responded, in substance, "Maybe . . . I think you should facetime me later when you get back, and we'll discuss it."

b. During the January 15 video chat, UC-1 asked SCHEININ what they would do when they met in person, and SCHEININ stated, in sum and substance, "I don't know; we'll figure it out." UC-1 responded, "but I like hearing about it." SCHEININ then stated, in sum and substance, "No. Because you're in public and shit." UC-1 then asked, "you still want to fuck?" and SCHEININ responded, "yeah. . . . Are you sure you can handle it?" UC-1 responded, in sum and substance, "only if you bring the lube."

c. During the January 15 video chat, UC-1 asked SCHEININ, in sum and substance, to bring Reese's peanut butter cups to the meet up. SCHEININ agreed and stated, in sum and substance, that UC-1 and SCHEININ can eat the candy together and have "Reese's peanut butter kisses. I don't know, that kind of sounds gross actually."

d. During the January 15 video chat, SCHEININ confirmed that they would meet at Location-1.

8. Based on my participation in this investigation, I am aware that SCHEININ arrived in the vicinity of Location-1 on January 16, 2020 at approximately 5:00 p.m. Soon after

his arrival at Location-1, agents placed SCHEININ under arrest. While conducting a search incident to arrest, agents found condoms and lubrication on SCHEININ's person.

B. Probable Cause Justifying Search of the Subject Premises

9. Based on my comparison of several of the video recordings of the Snapchat video chats between SCHEININ and UC-1 with a photograph of SCHEININ maintained in a law enforcement database, I believe that SCHEININ is the user of the SCHEININ Snap Username and the Scheinin Phone Number. Based on my review of information obtained from Snapchat pursuant to a grand jury subpoena, I am aware that at or around the time of UC-1 and SCHEININ's first Snapchat message exchange, on or about November 8, 2019, the SCHEININ Snap Username was accessed from a particular Internet Protocol ("IP") address (the "Target IP Address").² Based on my review of records obtained from the internet service provider ("ISP") for the Target IP Address, which records were obtained pursuant to a grand jury subpoena, I am aware that the Target IP Address was assigned to the Subject Premises on or about November 8, 2019 and that the account with the ISP was subscribed to in the name, "FREDERICK SCHEININ."

10. Based on law enforcement agents' review of records maintained by the DOJ-OIG, I am aware that SCHEININ listed the Subject Premises as his home address in materials submitted to the DEA.

² Based on my training and experience, I know that "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, meaning an Investigative Software assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. "Domain name" is a name that identifies an IP address.

11. Based on my participation in this investigation, including my review of text messages and video chat communications between UC-1 and SCHEININ, I am aware that SCHEININ regularly communicated with UC-1 through electronic means from the Subject Premises to engage in the Subject Offenses, including inducing and persuading UC-1 to transmit visual depictions of UC-1 engaging in sexually explicit conduct, whom SCHEININ believed to be a minor.

12. Based on my participation in this investigation and my conversations with other law enforcement officers, I am aware that individuals engaged in the Subject Offenses frequently keep paraphernalia in their homes, including: sex toys, condoms, lubricants, and candy.

C. Probable Cause Justifying Search of ESI

13. Based on my involvement in this investigation, I am aware that Google Voice and Snapchat can be accessed from various different electronic devices, including cellphones, computers, and tablets. As discussed above, SCHEININ has used electronic devices to commit the Subject Offenses from the Subject Premises. Therefore, I respectfully submit that there is probable cause to believe that the Subject Premises contains instrumentalities and evidence of the Subject Offenses, including SCHEININ's cellphones, computers, tablets, and other electronic devices that access the internet and records of communications between SCHEININ and UC-1 (or other minors) on those electronic devices.

14. Based on my training and experience, I know that individuals who engage in the Subject Offenses, including the production of child pornography and the enticement of minors to engage in illegal sexual activity, commonly use computers and other electronic devices to, among other things, communicate with victims, communicate with other individuals who engage in similar unlawful activity, solicit child pornography from others, maintain and store libraries of

child pornography for future exploitation. As a result, they often store data on their computers and other electronic storage devices, including external data storage devices, related to their illegal activity.

15. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is “deleted” on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in “slack space,” until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or “cache,” which is only overwritten as the “cache” fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user’s operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, CD-ROMs, or portable hard drives.

16. In addition to there being probable cause to believe that computer devices will be found on the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that these computers constitute instrumentalities of the Subject Offenses or constitute contraband subject to seizure, in that the computers may contain images depicting child pornography and/or communications with minors.

17. Based on the foregoing, I respectfully submit there is probable cause to believe that SCHEININ is engaged in the Subject Offenses, and that evidence of this criminal activity is likely to be found on computers and electronic media found in the Subject Premises.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

18. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Review of ESI

19. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under

government control) will review the ESI contained therein for information responsive to the warrant.

20. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “scanning” storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation³; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

21. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

³ Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

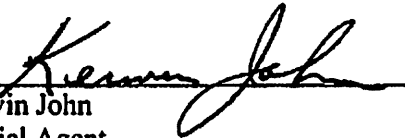
C. Return of ESI

22. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

23. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

24. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.


Kerwin John
Special Agent
Department of Justice, Office of Inspector General

Sworn to before me on
January 16, 2020


HON. RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the “Subject Premises”) are described as follows, and include all locked and closed containers found therein:

3-07 42nd Street, Apartment 3A, Sunnyside, New York, 11104, which is a multi-story residential apartment building located on 42nd Street, between 43rd Avenue and Queens Boulevard in Sunnyside, Queens (the “Building”). The building has a brick exterior with windows on each floor with the number “43-07” in gold writing affixed to the outside of the front entrance of the building. The Subject Premises is located on the third floor of the building. The entrance to the Subject Premises is a tan door with the alphanumeric characters “3A” affixed to it, which is accessible from the third floor hallway. A photograph of the entrance of the Subject Premises is depicted below:



II. Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (attempted production of child pornography), 2422(b) (attempted coercion and enticement of a minor to engage in illegal sexual activity), 2252A(a)(5)(B) (attempted possession of child pornography), and 2252A(a)(2)(B) (attempted receipt of child pornography) (the “Subject Offenses”) described as follows:

1. Evidence concerning occupancy or ownership of the Subject Premises, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Evidence concerning ownership, control, use of, or access to computer devices, storage media, and related electronic equipment used to access, transmit, or store information relating to the Subject Offenses.

3. The creation, content, and ownership of the Snapchat account username Zachs6015.

4. The creation, content, and ownership of the Grindr user identification zachs6015.

5. The creation or ownership of the telephone number 631-236-7220.

6. Communications with UC-1 between October 2019 and the present.

7. Evidence of other email accounts, social medial accounts, cloud storage accounts, or repositories of evidence concerning the Subject Offenses and passwords to access such accounts.

8. Images or videos depicting child pornography.

9. Evidence of attempts to download or otherwise receive child pornography or to visit websites on which child pornography is available between September 2019 and the present.

10. Communications with individuals aimed at enticing or persuading a minor to engage in illegal sexual activity between September 2019 and the present.

11. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from computer devices, storage media, and related electronic equipment.

12. Evidence reflecting registration of other online and social media accounts themselves potentially containing relevant evidence between September 2019 and the present.

13. Contraband associated with the Subject Offenses, including condoms, lubricant, sex toys, physical images depicting child pornography.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the Subject Premises also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment above, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras, data cards, CD-ROMs, DVD-ROMs, video game consoles, and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A and II.B of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.